CENTRO UNIVERSITÁRIO DE BRASÍLIA

Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

MÉTODOS E PRÁTICAS UTILIZADAS EM ENGENHARIA SOCIAL COM O INTUITO DE OBSTAR O ROUBO DE INFORMAÇÕES SENSÍVEIS.

Felippe Limongi Batista

2015

Felippe Limongi Batista

MÉTODOS E PRÁTICAS UTILIZADAS EM ENGENHARIA SOCIAL COM O INTUITO DE OBSTAR O ROUBO DE INFORMAÇÕES SENSÍVEIS.

Projeto apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como uma das atividades do programa de Metodologia Científica do curso de Pós-Graduação Lato Sensu na área de Redes de Computadores com Ênfase em Segurança

Orientador do Projeto: Prof. Me. Roberto Avila Paldês

Brasília

2015

Felippe Limongi Batista

MÉTODOS E PRÁTICAS UTILIZADAS EM ENGENHARIA SOCIAL COM O INTUITO DE OBSTAR O ROUBO DE INFORMAÇÕES SENSÍVEIS.

Projeto apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como uma das atividades do programa de Metodologia Científica do curso de Pós-Graduação Lato Sensu na área de Redes de Computadores com Ênfase em Segurança

Orientador do Projeto: Prof. Me. Roberto Avila Paldês

Brasília,___de_____de_____.

Banca Examinadora

_____

Prof. Msc. Francisco Javier de Obaldía Díaz

_____

Prof. Dr. Gilson Ciarallo

_____

Prof. Me. Roberto Avila Paldês

Dedico este trabalho aos meus pais, por sua capacidade
de acreditar e investir em mim.

“Dizem que pouco conhecimento é perigoso, mas não é nem a metade quanto muita ignorância”
-Terry Pratchett

RESUMO

A Engenharia social é uma técnica tão antiga e fácil de ser utilizada que pode ser muito perigosa. Esta pesquisa explica o que é a engenharia social. Como ela é entendida em todo mundo e porque o ser humano é tão vulnerável a ela. Como essa técnica pode explorar estas vulnerabilidades humanas. Quais são as principais técnicas que engenheiros sociais utilizam para conseguir que pessoas façam algo que a principio não queriam fazer? Como eles agem, quando agem, onde agem e por qual razão fazem o que fazem? Por que é tão difícil evitar esse tipo de ataque? Como pessoas comuns podem se defender contra engenheiros sociais e caso esses ataques venham acontecer, o que fazer para que o impacto não seja desastroso? Como profissionais da área de segurança da informação podem ajudar pessoas a entender a importância da segurança para suas companhias. A pesquisa foi fundamentada em bibliografias de autores consagrados sobre o assunto, pesquisas feitas por estudiosos das áreas de psicologia e ciência da computação e na própria experiência do autor. A pesquisa mostra como a ignorância sobre o assunto pode levar a perdas catastróficas para companhias.

Palavras-chave:

Engenharia social; Segurança da Informação; Vulnerabilidades;

1. INTRODUÇÃO

Hadnagy (2011) define engenharia social como qualquer ato que influencie uma pessoa a realizar uma ação que possa ser ou não de seu interesse. Com essa definição percebe-se que o engenheiro social pode utilizar-se de infinitas formas para alcançar seu objetivo.

Uma das técnicas de fazer das pessoas o alvo é conhecida como engenharia social. A engenharia social é uma mistura de ciência, arte e psicologia. Mesmo fazendo parte de três grandes áreas é uma técnica simples, porém extremamente efetiva e poderosa. A egenharia social é tão simples que todas as pessoas a utilizaram e a utilizam, mesmo sem saber ela está presente na vida de todos. Uma criança que chora quando seus pais não querem comprar seu brinquedo, um homem tentando conquistar uma mulher, empregado querendo um aumento e além disso,como qualquer outra ferramenta, a engenharia social pode ser utilizada para atividades criminosas.

Sabendo que o elo mais fraco de um sistema ou de uma organização não está protegido, atacantes utilizam pessoas como alvos para atingir seus objetivos, sejam eles informações bancárias de uma pessoa, dados secretos de um governo, informações sigilosas de uma empresa para vender ao concorrente ou até mesmo fotos de famosas nuas. *Hackers* usam pessoas porque o fator fraqueza humana é muito mais fácil de penetrar do que a fraqueza de uma rede.

Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda está vulnerável. (MITNICK; SIMON, 2006, p. 03).

Quando se fala em segurança da informação, logo associa-se a senhas, criptografia, *firewall*, antivírus, IPS/IDS, *hackers* e outros elementos de medidas defensivas técnicas. Raramente vinculamos segurança da informação a pessoas. Tendo em vista que a segurança da informação se mede pelo elo mais fraco, organizações estão sempre atrás do melhor *next generation firewall*, do melhor software para análise de *logs* e pacotes, gastando uma enorme quantidade de dinheiro em uma "falsa" segurança, pois no final, quem irá manter estes sistemas será o elo mais fraco, seres humanos.

Essa pesquisa irá focar em suas principais características dentro da ciência, analisando o ganho de informação, modelos de comunicações, elicitação e pretexto. Quanto à área da

psicologia, a pesquisa irá focar nos métodos de persuasão. Por fim, será exemplificado a arte que engenheiros sociais utilizam para unir as duas áreas visando atingir seus objetivos.

A crescente preocupação de organizações com a segurança da informação é perceptível, contudo estão em um caminho inexato. Hoje existe uma cultura global de que a segurança da informação é um simples módulo da área de TI, assim não englobando incidentes de segurança que ocorrem "fora de suas responsabilidades".

Quando se coloca pessoas vulneráveis a ataques de engenharia social, torna-se inviável restringir a segurança da informação somente dentro da TI, por isso a importância de ter uma nova mentalidade com segurança da informação englobando toda a organização.

Falando em organizações percebe-se que se tem um grande desafio. Quando fala-se em pessoas o problema é exponencialmente maior. Pelo simples fato da ignorância sobre o assunto, acreditam que ataques de engenharia social (isso quando sabem o que é engenharia social) nunca irão acontecer com eles.

Diante dos fatos apresentados, a pesquisa tem o intuito de responder o seguinte problema de pesquisa: Por que, mesmo com a melhor tecnologia de segurança da informação, os profissionais ainda estão vulneráveis a ataques de engenharia social? A pesquisa irá ajudar a complementar estudos feitos nessa área pouco explorada. Irá reunir vários estudos sobre áreas que faça parte da engenharia social.

Com isso o pesquisador, um profissional na área de segurança, vê-se na responsabilidade de aprofundar os conhecimentos atuais, com esta pesquisa e ajudar a mudar a mentalidade de pessoas e organizações, com um pouco mais de entendimento do mundo da engenharia social.

Para responder o problema da pesquisa o **objetivo geral** é conseguir entender métodos e práticas que engenheiros sociais utilizam para o roubo de informações sensíveis, a fim de evitá-las. Para tanto, foram estabelecidos os seguintes **objetivos específicos:** caracterizar o entendimento atual sobre engenharia social; entender técnicas utilizadas para esse tipo de ataque; e auxiliar na identificação e mitigação de ataques de engenharia social.

2. REFERENCIAL TEÓRICO

Para a pesquisa será realizado um levantamento bibliográfico de autores que escreveram sobre características da engenharia social, sobre métodos e práticas da psicologia social, como a psicologia social enquadra-se dentro da engenharia social e ao longo da pesquisa será feito um estudo de caso referenciando ao assunto tratado.

Em um primeiro momento, será tratado do conceito, dos métodos e das práticas que são base para o entendimento da engenharia social. Será utilizado um *quadro* conhecido como “The Social Engineering Framework" criado pela *social-engineer, inc*. Este quadro é construído separando partes das bases da engenharia social. Na primeira parte será apresentado como o termo engenharia social foi difundido.

O termo engenharia social ficou mais conhecido em 1990, através de um famoso *hacker* chamado Kevin Mitnick. Esse termo designa para práticas utilizadas a fim de se obter informações sigilosas ou importantes de empresas, pessoas e sistemas de informação, explorando a confiança das pessoas para enganá-las. Pode-se também definir engenharia social como a arte de manipular pessoas a fim de contornar dispositivos de segurança ou construir métodos e estratégias para ludibriar pessoas, utilizando informações cedidas por elas de maneira a ganhar a confiança delas para obter informações (SILVA, 2008).

Como já foi definido, engenharia social é qualquer ato que influencie uma pessoa a realizar uma ação que possa ser ou não de seu interesse (HADNAGY, 2011, p.10). Peixoto (2006, p. 4) diz: "Engenharia Social é a ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar segundo seu desejo. ” São conceitos bem parecidos, porem percebe-se que nestes dois conceitos os autores definiram engenharia social como uma técnica não criminal, sendo que é uma ferramenta poderosa que pode ser utilizada para qualquer fim.

Para outros autores, o conceito de engenharia social é visto tendo um lado de atividades ilegais, como a definição de Mann (2008, p. 19), quando ele diz que a engenharia social é o ato de manipular pessoas, enganando-as, para que forneçam informações ou executem uma ação.

Independente da ideia que autores tem sobre a engenharia social, é um senso comum que cada ataque de engenharia social é único tendo suas fases bem definidas. Allen (2006, p. 5) diz que cada ataque de engenharia social é único, com a possibilidade de envolver múltiplas fases/ciclos e/ou pode até mesmo agregar o uso de outras técnicas de ataque mais tradicionais para atingir o resultado final desejado.

Sobre as fases deste a ataque. Inicialmente o engenheiro social reúne o máximo de informações possíveis sobre a vítima, seguido pela criação de um tipo de relacionamento com a vítima, logo depois tem-se a exploração e a execução.

Geralmente o engenheiro social é um tipo de pessoa agradável. Ou seja, uma pessoa educada, simpática, carismática, mas sobretudo criativa, flexível e dinâmica e possui uma conversa bastante envolvente (ARAUJO, 2005, p. 27).

Quando se fala em vulnerabilidades de pessoas fala-se de psicologia, características que pessoas tem em comum que engenheiros social procuram explorar. Podemos destacar as seguintes características do ser humano que o torna vulnerável e suscetível a ataques de engenharia social (JUNIOR, 2006):

- vontade de se tornar útil: O ser humano procura ser cortês ou ajudar os outros quando necessário;
- buscar amizades: Os humanos costumam se sentir bem ao serem elogiados, de maneira que muitas vezes ficam abertos para fornecer informações;
- prorrogar responsabilidades: Muitas vezes o ser humano considera não ser o único responsável pelo conjunto de responsabilidades ou atividades;
- persuasão: É caracterizada pela capacidade de convencer, buscando assim a respostas desejadas para alcançar o objetivo. Isso acontece porque o ser humano possui características que o tornam vulnerável a manipulação.

Existem vários autores que já escreveram um pouco sobre a condição vulnerável que é o ser humano e o risco que isso traz para organizações quando não tem-se o devido cuidado com treinamento e concretização.

Os seres humanos são seres imperfeitos e multifacetados. Além disso, situações de risco modificam seus comportamentos, e, decisões serão fortemente baseadas em confiança e grau de criticidade da situação. (VARGAS, 2002 apud POPPER; BRIGNOLI, 2003, p. 7).

“ Eu não sou criptoanalista, nem matemático. Apenas sei como as pessoas cometem erros e elas cometem sempre os mesmos erros” (MITNICK; SIMON, 2005, p. 247).

Para explorar essas vulnerabilidades dos seres humanos existem inúmeras técnicas na área da psicologia social que são usadas por engenheiros sociais. Persuasão é uma delas. Para Kolenda (2013) os seres humanos são marionetes, anexado a cada um de nós existe um conjunto de cordas que, quando puxadas em uma determinada direção, guiam o nosso comportamento, sem a nossa consciência. Se você sabe como controlar as cordas, então você sabe como controlar o comportamento.

A persuasão é uma técnica que ajuda o engenheiro a moldar a decisão da vítima, sem que ela perceba e continue achando que aquela decisão tomada foi de sua vontade.

Como Ariely (2009) descreve, normalmente pensamos em nós mesmos sentado no banco do motorista, com controle total sobre as decisões que tomamos e a direção de nossas vidas; mas, infelizmente, esta percepção tem mais a ver com os nossos desejos, com a forma como queremos ver a nós mesmos do que com a realidade.

Outra técnica da psicologia muito poderosa utilizada para moldar decisões de pessoas, é conhecida como programação neurolinguística ou PNL. Segundo O'Connor e Seymour (2002 p. 2), A PNL é uma habilidade prática que cria os resultados que realmente queremos no mundo, criando valor para os outros no processo.

A PNL é um estudo revolucionário do processo do pensamento humano. Em outras palavras, é o estudo do que está realmente acontecendo quando pensamos. Não quero dizer reações físicas e eletroquímicas, mas o que notaria se olhássemos para as atividades passo-a-passo do pensamento (HOOBYAR; DOTZ; SANDERS, 2013, p. xxiii).

Em contexto da engenharia social utilizando a PNL, Hadnagy (2011) diz, NLP pode ensinar-te como usar sua voz, linguagem e escolhas das palavras para orientar as pessoas no caminho que você deseja.

Como dito anteriormente a engenharia social pode utilizar-se de várias técnicas, métodos e ferramentas. Não existe uma defesa contra a engenharia social, pode-se evitá-la com a conscientização e treinamento de pessoas.

"A verdade é que não existe uma tecnologia no mundo que evite o ataque de um engenheiro social" (MITNICK; SIMON, 2003, p. 195).

3. PROCEDIMENTOS METODOLÓGICOS

O método aplicado nesta pesquisa é o dedutivo, que segundo Gil (2008, p. 9) " é o método que parte do geral e, a seguir, desce para o particular. ". Ainda de acordo com Gil pode-se, com esse método, chegar a conclusões puramente formais, unicamente em virtude da sua lógica.

O método dedutivo é, também é conceituado por Lakatos e Marcone (1991, p. 92) da seguinte maneira:

> Tem o propósito de explicar o conteúdo das premissas. […]. Analisando sobre outro enfoque, diríamos que os argumentos dedutivos ou estão corretos ou incorretos, ou as premissas sustentam de modo completo a conclusão ou, quando a forma é logicamente incorreta, não a sustentam de forma alguma; portanto não há graduação intermediária.

Toda a parte conceitual da pesquisa foi estribado neste método. Com o reforço das informações técnicas e o embasamento teórico que abrangem o tema.

Para o procedimento foi adotado outros dois métodos, ambos em cada etapa da pesquisa, porém sempre havendo um predominante. Quando tratado das principais técnicas da engenharia social foi adotado o método monográfico, que segundo Gil (2008, p. 18) o estudo de caso em profundidade pode representar de muitos outros ou todos os casos semelhantes. Para Lakatos e Marcone (1991, p. 108) este método consiste no estudo de determinados indivíduos, grupos, instituições, com a finalidade de obter generalizações.

No momento em que foi tratado sobre os princípios psicológicos ligados a estas técnicas, o método predominante utilizado foi o observacional. Neste método Gil (2008, p. 16) conceitua da seguinte forma: pode ser tido como um dos mais modernos, visto ser o que possibilita o mais elevado grau de precisão nas ciências sociais. No estudo por observação apenas observa-se algo que acontece ou já aconteceu.

4. ANÁLISE E DISCUSSÃO DOS DADOS

4.1. Atual Entendimento da Engenharia Social

Engenharia social, apesar de ser uma prática bastante utilizada em todo o mundo e muito perigosa quando usada para fins maliciosos ou antiéticos, é pouco conhecida por essa definição, principalmente no Brasil. Segundo os poucos que já ouviram falar, muitos têm a definição errada do que se trata realmente a engenharia social.

Quando se diz que engenharia social é um pratica bastante utilizada, refere-se em cada uma de suas práticas que serão apresentadas posteriormente. São técnicas instintivas dos seres humanos, que muitas das vezes não sabem que estão praticando-as.

Esta prática é bastante perigosa pelo simples fato de ser pouco conhecida. Outro motivo de poder causar grandes danos é a sua facilidade com que as pessoas podem utilizar dessa técnica e alcançar altos objetivos.

Segundo o Dicionário Priberam da Língua Portuguesa o significado da palavra *engenharia* é "Conjunto de técnicas e métodos para aplicar o conhecimento técnico e científico na planificação, criação e manutenção de estruturas, máquinas e sistemas para benefício do ser humano”. “Ciência ou arte da construção”. Também define *social* como "Que diz respeito à sociedade. ”.

Combinando essas duas definições pode-se facilmente concluir que a engenharia social é a ciência ou arte de utilizar um conjunto de técnicas e métodos para aplicar o conhecimento técnico e cientifico no que diz respeito a sociedade. Sendo mais objetivo, utilizar os conjuntos de técnicas e práticas para manobrar seres humanos a realizares ações em alguns aspectos de suas vidas.

A engenharia social pode ser utilizada todos os dias de maneira quase imperceptível e não maliciosa. Pode ser utilizada por uma criança fazendo seus pais lhe darem algo que queira, um advogado tentando convencer um júri que seu cliente é inocente ou quem utiliza muito dessa técnica, muitas vezes de forma nada ética, são os políticos que fazem o que for possível para convencer eleitores a votarem neles. Policias e detetives também são pessoas que fazem o bom use desta, utilizando-a para conseguir informações de um determinado crime.

Trazendo a engenharia social para dentro da área de segurança da informação, geralmente envolve revelar certo tipo de informação ou ignorar controles de segurança dando acesso a lugares restritos ou a informações sigilosas. Para tal pode-se utilizar de várias formas desde uma simples porta deixada aberta por um funcionário desatento ou ataques sofisticados como passar muito tempo colhendo informação para torna-se um funcionário de uma companhia que seja seu alvo e então roubar informações valiosas.

Com o avanço da tecnologia, tanto em softwares e hardwares de segurança, achar uma vulnerabilidade fica cada vez mais complicado, por isso atacantes cada vez mais estão combinando suas habilidades técnicas com métodos da engenharia social para tornar seus ataques mais fácil e eficientes. Grande parte dos ataques que se ouve falar inclui algum elemento da engenharia social, porém não é reportado. Na maioria das vezes quem sofre desses tipos de ataques não percebem que foram vítimas da engenharia social, sabendo que um ataque deste tipo é muito difícil de ser detectado. Quando percebem que sofreram um ataque de engenharia social, ficam envergonhados em reportar o acontecido. Isso por pensar que pode parecer culpado ou com medo de perder a credibilidade.

Conforme a SOCIAL ENGINEER, INC em seu framework, bons engenheiros sociais são especialistas no comportamento dos seres humanos. Eles conseguem perceber com facilidade onde encontram-se suas fraquezas e explora-las. Conseguem manipula-las e engana-las com pouco esforço. Pessoas são curiosas e preocupadas, adoram coisas de graça e sentir-se mais importante que outros, nunca imaginam que podem estar sendo vítimas de algum tipo de ataque.

Para um profissional da área de segurança torna-se árduo trabalhar contra isso, pois além de lutar contra a natureza humana segurança da informação é trabalhoso e dificil para o usuário final. Por exemplo. Ter senha com no mínimo 8 caracteres sendo que deve possuir letras maiúsculas, letras minúsculas, números e caracteres especial e trocar a cada 90 dias é muito complicado. Uma das melhores maneiras para mudar a mentalidade das pessoas é provar que isso acontece, e acontece com todos. Demonstrar em ambiente controlado que pode acontecer com elas e consequentemente acontecer com a empresa onde ela está.

Seres humanos são, sem dúvida, o elo mais fraco em todas as organizações. Engenheiros sociais sabem disso e exploram essa falha. Para defender contra esse tipo de ataque é necessário conhecer sobre a natureza humana, o que permite que engenheiros sociais utilizam um conjunto de técnicas para enganar pessoas.

(CONHEADY, 2014, p.53) cita confiança, medo de autoridades, desejo de ser útil, falta de preocupação com a segurança como algumas das razões que fazem a engenharia social funcionar com pessoas em qualquer lugar do globo. Abaixo será detalhada cada uma.

4.1.1. Confiança

Desde pequenos somos educados a confiar nas pessoas próximas, vizinhos, colegas de escola, colegas do trabalho. Está na natureza humana a confiança nas pessoas. Isso é a principal razão da engenharia social funcionar. A sociedade em que vivemos é baseada em confiança.

Confiar nas pessoas não é uma tarefa muita fácil. Na maioria das vezes pessoas são quem elas dizer ser. É raro pensar que uma pessoas está tentando enganar alguém, embora sempre nos deparamos com pessoas vigaristas, fraudadores ou engenheiros sociais. É fácil acreditar em um engenheiro social dizendo que ele é um pessoa que diz ser sem nem sequer pedir um documento que prove o que está dizendo. Algumas pessoas são simplesmente mais confiáveis que outras por falar bem, por vestir bem, por ter informações sobre um pessoa que você já confia, enfim os motivos são inúmeros.

No ambiente de trabalho torna-se mais fácil confiar nas pessoas, pois estão dentro do mesmo grupo, as vezes por imaginar que essa tem autorização ou o pedido veio de uma autoridade superior ou por querer finalizar o trabalho de forma mais rápida ou simplesmente gostar da pessoa.

Um estudo (The Nature anda Effects of Young Children's Lies) realizado pela Universidade de Waterloo, em Ontário, no Canadá, observou que crianças de 4 anos de idade mentem a cada 2 horas, enquanto uma criança de 6 anos conta um mentira a cada 90 minutos. Crianças aprendem desde cedo a mentir para encobrir coisas erradas que fizeram. Um comportamento tipicamente normal. Na verdade os pesquisadores descobriram que o complexo processo que envolve mentir está diretamente ligada a inteligência. Pessoas adultas ficam cada vez mais habilidosos na arte de mentir. Este estudo também mostrou que 25 porcento das relações interpessoais envolve mentiras. Por isso o perigo de confiar tanto nas pessoas.

Outro ponto que faz com que a engenharia social seja uma arma poderosa nas mãos de pessoas mal intencionadas é a dificuldade que pessoas tem em detectar uma fraude. Pessoas querem acreditar no que estão ouvindo é verdade. Em um estudo, conhecido com "Project Wizard" realizado pela Universidade da California, São Francisco, e liderado pelos psicólogos Paul Ekman e Maureen O'Sullivan gastaram mais de 20 anos estudando sobre habilidades que pessoas possuem em detectar mentiras. Suas pesquisas mostraram que a maioria das pessoas somente conseguem detectar algo em torno de 50 porcento das vezes. Mostraram também que

indivíduos treinados para esse tipo de situação como, policias, psiquiatras não se saem melhor
.

Foram mais de 15 mil pessoas participantes dos estudos. Os pesquisadores conseguiram identificar somente 50 pessoas do total com uma habilidade excepcional em detectar mentiras, os quais foram chamados de “verdadeiros magos”. em seus estudos comprovaram que um “verdadeiro mago” consegue identificar uma mentira 80 porcento das vezes. Contudo, nem um “verdadeiro mago” conseguiu atingir a marca de 100 porcento. Partindo deste principio: se até eles podem ser enganados por um engenheiro social, imagina pessoas comuns.

Uma das grandes vantagens que engenheiros sociais tem é parecer pessoas confiáveis. Existem vários estudos sobre quais caracterizas tornam as pessoas mais confiáveis. Um estudo chamado “ A Voice Is Worth a Thousand Words: The Implications of the Micro-coding of Social Signals in Speech for Trust Research.” nos mostra que pessoas que possuem um tom de voz mais baixo são consideradas mais confiáveis e mais inteligentes. Um outro estudo que mostra como caracteristicas podem ajudar a influenciar pessoas é “Trustworthy-Looking Face Meets Brown Eye” diz que pessoas com olhos castanhos são mais confiáveis do que pessoas com olhos azuis.

Mais do que qualquer coisa confia-se nas pessoas que são similares e que possuem o mesmo gosto, mesma visão política, mesma religião, mesmo sexo, mesmo time de futebol. Assim para um engenheiro social sabendo disso, fica fácil mentir para uma pessoa dizendo que tem os mesmo gostos para conquistar sua confiança.

4.1.2. Medo de Autoridades

Desde o momento em que nascemos, estamos condicionado a respeitar quem tem autoridade, começando por pais, passando por professores, chefes, policias e geralmente pessoas com uniformes. A maioria das pessoas tendem a obedecer uma autoridade inquestionavelmente. Se uma pessoa com algum uniforme de policia, por exemplo, pedir que esta pessoa faça algo, provavelmente essa pessoa ira realizar.

Pessoas tendem a cumprir algum pedido feito por pessoas que parecem estar em posições autoritárias. Sabendo disso o engenheiro social utiliza desse fato se passando por alguma pessoa com algum tipo de autoridade para atingir seus objetivos. Obediência envolve uma hierarquia de poder e status, então quando um atacante utiliza a engenharia social para fazer um pedido como uma pessoa de alto status, muito provavelmente esse pedido sera cumprido.

Além de se passar por uma pessoa com autoridade, o engenheiro social pode ser mais convincente caso consiga usar um uniforme. Assim, aumentando a chance de ser visto como alguém que realmente merece ser respeitada e seus pedidos atendidos. Alguns fatores aumentam a tendência das pessoas obedecerem.

- **Autoridade:** Pessoas são mais propensas a obedecer autoridades com credibilidade. com isso o engenheiro social com um uniforme de um policial, engenheiro de uma empresa ou até mesmo um zelador, podem conseguir acesso a um lugar restrito.
- **Pressão:** Pessoas obedecem com mais facilidade quando estão sobre pressão e não possuem ajuda. Esta é uma das razoes que engenheiros sociais aproveitam para colocar a vitima sobe pressão para realizar uma tarefa com rapidez.
- **Justificativa:** Pessoas irão provavelmente obedecer mais se acreditarem que estão fazendo aquilo por uma boa causa.

4.1.3. Desejo de Ser Útil

Pessoas gostam de ajudar, sentem-se bem ajudando o próximo. Pessoas geralmente sente-se compelida em ajudar outras pessoas, até estranhos, principalmente dentro do ambiente de trabalho. Algumas pessoas, tem em seus trabalhos a função de ajudar outras pessoas, relação com o cliente, help desk, call center e recepcionista, são alguns exemplos. Geralmente são essas pessoas os primeiros alvos dos engenheiros sociais porque é o trabalho deles passar informação.

Para piorar a situação, muitas vezes pessoas ajudam outras pessoas sem o pedido de ajuda. segurar um porta para uma pessoa com as mãos ocupada acontece com frequência. Se alguém pedir uma ajuda direta é quase que impossível alguém negar.

Carnegie (2012, p. 139), um mestre na área d relacionamento com pessoas, em seu livro, *Como Fazer Amigos e Influenciar pessoas*, mostra-nos uns dos princípios para torna-se uma pessoa mais amigável é: “Faça a outra pessoa sentir-se importante, e faça-o com sinceridade. Um engenheiro social quando pede ajuda para alguém e consegue provar para essa pessoa que ela o ajudar ele irá considera-la um pessoa importante é quase certo que essa pessoa irá o ajudar sem pensar duas vezes.

4.1.4. Falta de Preocupação com a Segurança

Frequentemente a engenharia social funciona porque pessoas não se dão conta de que isso é um problema. E mesmo quando percebem que é uma ameaça acham que não é nada demais e que não precisam alertar ninguém.

Com o crescimento das redes sociais a vida dos engenheiros sociais tornou-se mais fácil, pois basta entrar no perfil do facebook de alguém e colher inúmeras informações sobre a vitima. Ataques se tornam mais sofisticado quando se tem uma grande quantidade de informação pessoal. Mas por qual motivo as pessoas colocam uma quantidade enorme de informações pessoais na internet?

Muitas pessoas não sabem da existência da engenharia social. Quando percebem que foram atacados não se dão conta que foi um ataque desse tipo. Um dos ataques de engenharia social mais conhecido é o de phishing e em seu surgimento na década de 90 fez incontáveis vitimas em todo o mundo, pois era totalmente desconhecido por todos. Hoje ainda phishing faz suas vitimas, mas seus ataques são mais direcionados a uma vitima em especifico.

Um dos grandes pesadelos para um profissional de segurança da informação é ouvir uma pessoa dizendo que não está preocupada com isso pois não tem nada a perder. Isso é um pensamento muito arriscado, pois se a pessoa não acredita que não tem motivos para ser um alvo não irá tomar as precauções necessárias para sua segurança.

Das poucas pessoas que sabem o que é a engenharia social e se preocupa com ela, muitas não sabem o que fazer quando estão diante de uma situação dessas e quando tentam fazer algo, na maioria das vezes agem de forma errada.

4.2. Técnicas utilizadas pra esse tipo de ataque

Foi visto um entendimento atual do que é a engenharia social e porque ela funciona tão bem e é tão perigosa. Nessa secção será discutidos as técnicas que segundo Hadnagy, 2011 são utilizadas por engenheiros sociais para conseguir explorar vulnerabilidades das pessoas que foram discutidas acima.

4.2.1. Coleta de informações

Quando é falado de informação para a engenharia social não existe informação que seja irrelevante. Qualquer informação, por mais insignificante que uma pessoa possa achar ser, para um engenheiro social pode ser a chave para o sucesso de um ataque.

Pode-se comparar a coleta de informação com uma construção de uma casa. Se tentar começar pelo teto a casa nunca irá terminar. Assim como a casa a coleta de informação segue o mesmo principio deve sempre coletar as que pode ser encontrada com facilidade. desse jeito terá uma boa base de conhecimento, na analogia com a casa seria mesmo que dizer uma boa fundação.

Existe, hoje, vários meios de coleta de informações que varia desde vasculhar o lixo da empresa instalar algum spyware no computador do diretor de um companhia, passando por espionagem com binóculos e escutas telefônicas.

Na coleta de informações geralmente o engenheiro social consegue um numero alto de informações, para depois, com a parte difícil que será organiza-las para conseguir algo que possa ser útil. Sempre deve-se pensar como um engenheiro social. O engenheiro social sempre pergunta sobre tudo, atento aos detalhes.

Como dito anteriormente fontes para coleta de informações é inesgotável então torna-se impossível falar sobre todas, mas será apresentadas algumas:

- Websites: Sites de companhias ou mesmo sites pessoais são excelentes formas de conseguir informasse sobre um alvo. Saber sobre o que fazem, produtos ou serviços que oferecem, locais, numero para contato e até o linguajar que é utilizado.
- Ferramentas de busca: Google, como não falar dele. Pode-se dizer que é o grande amigo do engenheiro social. O google permite que pessoas utilizem operadores avançados para realizar um busca mais detalhadas. Por exemplo, se for utilizado “inurl:admin inurl:usuarios filetype:php ”. Irá trazer uma pagina php de usuário com privilegio de adminitrador onde controla contas de usuário, caso a pagina não tenha uma segurança o engenheiro terá acesso a todas informasse de usuário de um site. Sabendo perguntar para o google ele pode te responder quase qualquer coisa.

- Rede sociais: Considerado hoje por muitos uns dos maiores riscos para a segurança de uma pessoa ou um companhia estão as redes sociais. Facebook, instagram, Twitter, LinkedIn e etc. informações sobre pessoas estão a mostra na internet para todo o mundo ver. Com facebook de uma pessoa pode-se descobrir gostos, o que a pessoa faz, onde trabalha, onde estuda, amigos, família, tudo.
- Observar: Um engenheiro social é no mínimo um observador, curioso, quer saber de tudo. Observar pessoas, saber como as pessoas de um empresa se comportam, se vestem, usam crachá, como falam, como se tratam. Tudo isso pode ajudar o atacante a conseguir maneiras de entrar em um prédio ou mandar um email para o diretor de um empresa sobre promoção de uma viagem para um lugar que descobriu em o diretor sempre quis visitar.
- Lixo: Muitas empresas não dão valor necessário ao descarte das informação. No ciclo da segurança da informação. Após classificar um informação ela deve ter o mesmo nível de segurança desde da criação, transporte, uso, armazenamento e descarte.

4.2.2. Elicitação

Elicitação pode ser considerada umas das técnicas mais importantes e criticas da engenharia social. Ela pode glorificar ou acabar com um ataque de um engenheiro social.

Pessoas já se depararam com alguém que acabaram de conhecer, mas já sentiriam uma grand afinidade por ela e não sabem por quê. Isso pode ser natural de uma pessoa mas isso tem nome, elicitação.

Elicitação é saber conversar, ser educado, saber se vestir, para conquistar a confiança das pessoas saber fazer perguntas inteligentes para receber respostas certas. Elicitação é tão poderosa que muitos governos educam e alertam seus funcionários sobre essa técnica, pois é utilizada por espiões em todo mundo.

Um engenheiro social quer que sua vítima execute uma ação determinada. Executar uma ação pode ser responder um pergunta ou dar acesso a uma área restrita. Para conseguir tal feito o engenheiro irá conversar com sua vitima, prender sua atenção, conquistar sua confiança para que ele realize seu desejo.

O porquê da elicitação ser tão poderosa é porque ela não é uma ameaça é uma simples conversa. Quantas vezes por dia pessoas não tem uma pequena conversa com um desconhecido na fila de um banco em um restaurante, no trabalho, em qualquer lugar. Toda a metodologia da elicitação é segurar a pessoa na conversa e uma conversa não maliciosa.

Hadnagy (2011, p. 59) cita três elementos que são considerados essenciais para arte da conversação, são eles:

- Relaxe: Nada é pior para uma conversa do que uma pessoa não estar confortável com o assunto em questão. Quando uma pessoa conhece um assunto ela fica confortável sua linguagem corporal é diferente é tranquila e o assunto flui sem problemas. Agora quando uma pessoa começa a falar sobre algo que não tem conhecimento a postura corporal é outra a pessoa fica retraída a língua trava e a conversar parece mais uma entrevista do que uma conversa amigável. Para conseguir ter uma conversa amigável o próximo elemento existe.
- Eduque-se: Sim, estudar! O bom engenheiros social deve ter conhecimento sobre o assunto que está conversando com sua vítima. Uma coisa muito importante salientar nesta etapa é imprescindível do engenheiro não fingir que saiba mais do que ele realmente saiba. Um exemplo, caso um engenheiro queira descobrir informações de um desenvolvedor sobre códigos novos de um software secreto. Ele somente irá apresentar-se como um desenvolvedor somente se ele tiver realmente conhecimentos sobre o assunto, caso contrario o desenvolvedor irá perceber que ele não sabe de nada e a conversa irá encerrar.

  Não importa qual seja o assunto, um bom engenheiro social irá realizar pesquisas, praticar e estar preparado para a conversa. Ter conhecimento suficiente para ter uma conversa inteligente com a vitima irá chamar sua atenção.
- Controle-se: O grande objetivo final da elicitação é conseguir respostas. Mas um engenheiro social nunca irá conseguir tais respostas caso comece a fazer varias perguntas de uma vez sobre o que deseja. Como dito na primeira etapa, seja natural. Deixar a pessoa falar, contar suas historias, na maioria da vezes é o melhor a se fazer. Muitas das vezes pessoas que são taxadas como “Boas conversadoras” geralmente escutam mais do que falam.

4.2.3. Pretexto

Pretexto no contexto da engenharia social, para alguns, é somente contar uma historia ou uma mentira para ser encenada durante a ação do engenheiro social, mas para outros a definição de pretexto é um pouco mais do que isso. Pretexto pode ser definido como uma historia de fundo, personalidade e atitudes para maquiar um engenheiro ajudando-o a enganar sua vitima.

Pretexto irá maquiar totalmente o que o engenheiro social é de verdade, tudo com um bom pretexto fica praticamente impossível descobrir se o engenheiro é uma mulher ou homem, se é rico ou pobre, se mora perto ou em outro pais, enfim quanto melhor o pretexto mais convincente será o engenheiro social.

Com a internet o pretexto ficou cada vez mais fácil de se fazer, logo pessoas com intenções maliciosas utilizando essa técnica também aumentou. Todo mundo já ouviu historias como de pedófilos se passando por crianças na internet para atrair outras crianças, pretexto para o mal e do

outro lado agentes das forças policias se passando também por crianças para atrair pedófilos. Pretexto como qualquer outra feramente pode ser utilizada para ambos os fins.

Pretexto então pode ser visto como a arte de criar um cenário para persuadir alguém e conseguir obter algum tipo de informação. Não somente criar uma mentira, mas atuar como uma nova pessoa, viver o personagem. O próprio engenheiro social deve acreditar em seu próprio cenário para que sua atuação seja mais convincente.

4.3. Identificar e Mitigar Ataques

Para chegar até aqui, foi mostrado na pesquisa vulnerabilidades que engenheiros sociais exploram e técnicas que eles utilizam para tal. Quando pessoas começam a entender o que é a engenharia social de verdade e percebem o quanto ela é poderosa seus sentimentos são de impotência e medo. Tudo piora quando é dito que não existe uma fórmula 100% garantida para evitar ataques de engenharia social.

Mais uma vez, não há uma defesa 100 porcento contra este tipo de ataque. Porém ele pode ser mitigado e até evitado. Caso venha acontecer e se a vítima estiver preparada com certeza a resposta será mais eficiente e causando o menor prejuízo possível.

É notória a dificuldade em se defender contra esse ataque porque são direcionados ao elo mais fraco da segurança da informação, seres humanos. Seres humanos não são como maquinas que são configuradas ou atualizada para não serem mais vulneráveis a engenharia social.

A primeira maneira de evitar um ataque desse tipo é a identificação de possíveis alvos. Sendo um responsável pela segurança de um empresa e conhecendo como um engenheiro social trabalha é possível perceber pelo comportamento de algumas pessoas que seriam alvo fácil. O profissional deve pensar como um atacante e coloca-se no lugar dele.

Outra parte importante é identificar o engenheiro social e de acordo com Hadnagy (2011) existem algumas categorias que podem ajudar a encontra-lo antes que cumpra seus objetivos.

- Atitudes: como um pessoa com um extremo bom humor até demais, muito carinhosa muito educada, muito paciente, querendo ajudar demais. Pessoas desconhecidas com pedidos autoritários. Talvez com um extremo mal humor, pedindo para realizar coisas agressivamente. Ou até mesmo sendo muito emocional, chorando demais ou fincando muito chateada com alguma coisa.
- Tentativa de conexão: Tentar estabelecer uma conexão com suas vitimas é uma tarefa importante para os engenheiros sociais. Usar nomes de pessoas conhecidas sendo que a tal pessoa nunca te falou do atacante. Agir particularmente amigável e até usar informasse pessoais sobre a vitima.

- Pequenos erros: Mesmo que engenharia social seja uma técnica bastante eficiente, ser um bom engenheiro exige experiência e muita técnica. Sabendo disso engenheiros menos experientes comentem muitos pequenos erros, as vezes despercebidos aos olhos de uma pessoa comum, mas para alguém que já conhece suas técnicas pode ser suficiente para evitar o ataque.

Além de conseguir identificar possíveis vitimas e engenheiros sociais, não existe formula melhor para evitar esse tipo ataque do que o conhecimento. Saber o que é a engenharia social, entender como funciona, saber das fraquezas que o seres humanos possuem isso, informar as pessoas do que se trata isso pode diminuir significativamente o ataque de engenharia social.

Sempre conferir se os dados que uma pessoa apresentou conferem com o real. Pedir a carteira de identificação, conferir o crachá da pessoa para ter certeza que ela pode ter aceso aquele lugar. Conferir com alguém superior se o pedido daquela pessoa é verdadeiro.

A educação e avisos dentro de uma empresa pode salva-la. Isso é de responsabilidade do profissional de segurança. Ele tem o dever de convencer superiores da importância em dar cursos, workshops, newsletters, posters, etc. Tudo tem algum valor contra a engenharia social.

Outro importante dever do profissional de segurança é atualização da política de segurança de uma companhia. Deixar claro de como tudo dentro daquela empresa funciona. O que pode e que não pode. E sempre deixar procedimentos bem explicados, detalhados do que fazer caso algum tipo de ataque venha a acontecer.

5. Conclusão

Ataques de engenharia social estão limitados apenas pela imaginação do engenheiro social. Existem centenas de exemplos deste tipo de ataque e as razões para esses ataques são infinitas. Foi observado como e porque esses ataques funcionam tão bem com qualquer tipo de pessoa em qualquer lugar do mundo. Esta pesquisa mostra razões da natureza humana que torna o homem um ser vulnerável o que facilita os ataques.

Esta pesquisa teve o cuidado de exemplificar como os engenheiros sociais exploram as vulnerabilidades humanas. Como utilizam destas técnicas para poderem alcançar seus objetivos sendo que às vezes as vitimas não se dão conta de que foram atacadas. Foi mostrado também como um engenheiro social pode aproveitar tudo que está em seu redor para atacar, e como a ignorância pode ser perigosa para pessoas e companhias.

Muitos estudiosos de psicologia têm passado anos de suas vidas estudando diferentes aspectos do ser humano, do comportamento humano. Alguns desses estudos ajudam a entender como e porque é tão fácil para um bom engenheiro social enganar uma pessoa com tamanha facilidade. Todos são humanos, portanto, na maior parte, são previsíveis. Todos são diferentes. Seres humanos não são como máquinas, cada um possui um sentimento, cultura, tudo muda, embora a engenharia social consiga obter um padrão em suas vidas.

Conseguir anular completamente um ataque de um engenheiro social experiente e determinado é quase impossível. Por isso, os melhores e mais avançados softwares e hardwares do mundo são inúteis caso os seres humanos que estão em sua administração não tenham conhecimento sobre a engenharia social. Serão enganados facilmente e no pior dos casos irão dar informações sigilosas para o atacante sem perceber.

Para o profissional da área de segurança da informação, prevenir que casos como esses ocorram se torna muito complicado. Porque além de se proteger tem que convencer a outra pessoa o quanto a segurança é importante. É necessário entender como os engenheiros sociais trabalham, como eles fazem e porque fazem. Confiar nas pessoas é necessário, mas não custa nada checar se as informações passadas são verdadeiras. Como um provérbio russo famoso dito pelo ex presidente dos Estados Unidos, Ronald Reagan, na assinatura do *Tratado INF* em 8 de dezembro de 1987 “Confie, mas verifique”.

Umas das maiores limitações dessa pesquisa foi a baixa quantidade de estudos brasileiros relacionados a esse assunto. Existem várias reportagens sobre engenharia social, porém sem aprofundar no assunto. Artigos são quase inexistentes. Estudos de outros países, principalmente da língua inglesa existem vários, por isso a pesquisa focou nessas fontes de pesquisas.

Para trabalhos futuros pode-se focar em aprofundar em características abordado nesta pesquisa. Etapas utilizadas por engenheiros sociais para conseguir informações podem ser aprofundadas para entender melhor como funcionam. Pode ser usado para estudos sobre a psicologia social, utilizada na engenharia social.

6. REFERÊNCIA

ALLEN, Malcolm. Social Engineering: A Means to Violate a Computer System. **SANS Institute InfoSec Reading Room.** june./dec. 2006. Disponível em: <http://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529>. Acesso em: 17 set. 2014.

ARAUJO, Eduardo E. de. **A VULNERABILIDADE HUMANA NA SEGURANÇA DA INFORMAÇÃO**. 2005. 85 f. Monografia (Graduação)– Faculdade de Ciências Aplicadas de Minas, União Educacional Minas Gerais S/C LTDA, Uberlândia, 2005. Disponível em: . Acesso em: 16 out. 2014.

ARIELY, Dan. **Predictable Irrational** The Hidden Forces That Shape Our Decisions. New York, NY: HarperCollins Publishers, 2008.

CARNEGIE, Dale. **Como fazer amigos e Influenciar Pessoas:** O guia clássico e definitivo para relacionar-se com as pessoas. 52 ed. São Paulo: Companhia Editora Nacional, 2012.

CONHEADY, Sharon. **Social Engineering in IT Security:** Tools, Tactics, and Techniques. Estados Unidos: McGraw-Hill Education, 2014.

EKMAN, Paul; O'SULLIVAN, Maureen. **Lying and Deceit** - The Wizards Project. Disponível em: <http://www.eurekalert.org/pub_releases/2004-10/ama-lad100804.php>. Acesso em: 12 dez. 2014.

GIL, Antonio Carlos. **Métodos e Técnicas de Pesquisa Social**. 3 ed. São Paulo: Atlas,2008

HADNAGY, Cristopher. **Social Engineering:** The Art of Human Hacking. Indianapolis, IN: Wiley Publishing, 2011.

HOOBYAR, Tom; DOTZ, Tom; SANDERS, Susan. **NLP:** The Essential Guide. New York, NY: HarperCollins Publishers, 2013.

JUNIOR, Guilherme. **Entendendo o que é Engenharia Social**. 2006. Disponível em: <http://www.vivaolinux.com.br/artigo/Entendendo-o-que-e-Engenharia-Social>. Acesso em: 17 set. 2014.

KLEISNER, K., PRIPLATOVA, L. FROST, P., FLEGR, J. **Trustworthy-Looking Face Meets Brown Eyes**. 2013. Disponível em:

<http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0053285> Acesso em: 20 fev. 2015.

KOLENDA, Nick. **Methods of Persuasion**: How to use psychology to influence human behavior. Kolenda Entertainment, 2013.

LAKATOS, Eva Maria; MARCONI, Marina A. **Fundamentos de Metodologia Científica**. 3ª Ed. São Paulo: Atlas, 1991.

MANN, Ian. **Engenharia Social.** São Paulo: Edgar Blücher, 2008.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar**: Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson Education, 2006.

MITNICK, Kevin D.; SIMON, William L. **The art of intrusion**: the real stories behind the exploits of hackers, intruders, and deceivers. Indianapolis: Wiley Publishing, 2005.

O'CONNOR, Joseph; SEYMOUR, John. **Introducing NLP**: Psychological Skills for understanding and Influencing People. San Francisco, CA: Red Wheel/Weiser, 2011.

PEIXOTO, Mário C. P. **Engenharia Social e Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006.

POPPER, Marcos Antonio; BRIGNOLI, Juliano Tonizetti. **ENGENHARIA SOCIAL**: Um Perigo Eminente. [2003]. 11 f. Monografia (Especialização)– Gestão Empresarial e Estratégias de Informática, Instituto Catarinense de Pós-Graduação – ICPG, [2003]. Disponível em: . Acesso em: 19 set. 2014.

PRIBERAM, Dicionário da Língua Portuguesa, 2008-2013. Disponível em <http://www.priberam.pt/DLPO/social. Acesso em: 20 fev. 2015>

SILVA, Elaine M. da. **Cuidado com a engenharia social**: Saiba dos cuidados necessários para não cair nas armadilhas dos engenheiros sociais. 2008. Disponível em: <http://www.tecmundo.com.br/msn-messenger/1078-cuidado-com-a-engenharia-social.htm> Acesso em: 17 set. 2014

SOCIAL ENGINEER, INC. **The Social Engineering Framework.** Disponível em: <http://www.social-engineer.org/framework/general-discussion> Acesso em: 18 nov. 2014.

WABER, B., WILLIAMS, M., CARROL, J., PENTLAND, A. **A Voice Is Worth a Thousand Words:** The Implications of the Micro-coding of Social Signals in Speech for Trust Research. 2012. Disponível em: <http://digitalcommons.ilr.cornell.edu/articles/905>. Acesso em: 21 fev. 2015.

WILSON, Anne E; SMITH, Melissa D; ROSS, Hildy S. **The Nature and Effects of Young Children's Lies.** 2003. Disponível em: <http://onlinelibrary.wiley.com/doi/10.1111/1467-9507.00220/abstract>. Acesso em: 18 fev. 2015.